REMARKS

This is a full and timely response to the non-final Office Action mailed September 11, 2007. Reconsideration and allowance of the application and presently pending claims are respectfully requested.

Present Status of Patent Application

Claims 1-30 are pending in the present application. Specifically, claims 1-30 are original unamended claims. Reconsideration and allowance of the application and presently pending claims are respectfully requested.

Summary of Examiner interview

Applicants wish to thank Examiner Johnson and Supervisor Moazzami for the phone conversation conducted on November 5, 2007 wherein Applicants' representatives discussed the current Office Action with reference to pending claims. No specific conclusions were reached.

Claim Rejections under 35 U.S.C. §102

Statement of the Rejection

Claims 1-14, 17-27, 29, 30 are rejected under 35 U.S.C. 102(e) as being anticipated by Yan et al. (US PGPUB No. 20050033987).

Response to the Rejection

Claim 1

As is known, a proper rejection under 35 U.S.C 102 necessitates that the cited prior art reference must teach every aspect of the claimed invention with no question of obviousness being present. Applicants respectfully submit that the current rejection of claim 1 under 35 U.S.C 102 fails to satisfy this requirement because the cited prior art of Yan fails to unambiguously disclose each aspect of claim 1.

Applicants' claim 1 pertains to establishing a trust-based relationship between two entities. Towards this end, a first entity constructs an attestation message containing various security parameters (code ID, digital signature, certificate, verifiable by a security key etc.)

that is transmitted to the second entity. The second entity decides whether to enter into the trust-based relationship after receiving the attestation message. Upon deciding to do so, the second entity informs the first entity by transmitting a trust message containing a secret that is to be shared between the two entities for ensuring secure communication from thereon.

In contrast, the cited prior art of Yan discloses a relationship based on a conditional trust that is initially established between a trustor and a trustee (challenge 302 and response 304 of FIG. 3), after which the trustee sends out a "distrust" message (message 314) whenever there is a "condition change" in the trustee that poses a threat to the conditional trust.

Specific attention is drawn to Yan's Background section (paragraphs [0006] and [0009]), which outlines certain "limitations in the prior art" and is reproduced below for convenient reference:

> [0006] The way in which a remote computing platform can be trusted is as follows. First, integrity metrics are queried from the platform, which are digitally signed by the trusted component of that platform. Second, the integrity metrics are compared with expected values that represent components that are trusted enough to perform the intended purpose. Third, if the compared values match the expected values, trusted interaction with the remote computing platform may be commenced.
>
> [0009] Since trust is dynamic, it is impossible to provide a static/absolute trust solution. Accordingly, one disadvantage of the current TCPA paradigm, is that it does not provide a dynamic solution and is thus unable to tailor its protection for the changeable trust component. The static nature of the current TCPA solution, therefore, may cause a waste of resources and unnecessary attestation when the trust level is actually very high, while failing to satisfy security requirements for transactions when the trust level is actually very low.

In order to overcome the above-described "limitations in the prior art" Yan proposes a solution that is based on "distrust signals" and described in his Abstract section as follows:

> A system and method is provided that establishes and maintains conditional trust by stating a signal of distrust from a trustee's computing platform to a trustor's computing platform. The trustor attests a trustee at a given time and also sends trust conditions to the trustee upon which the trustor trusts the trustee for some intended purpose. The trust conditions may include restrictions on hardware or software components and any status changes to the hardware or software components. The trustee then monitors the hardware and software components in relation to the trust conditions and reports distrust signals when the trustee's hardware and software configuration no longer

matches the trust conditions. (Emphasis added)

As mentioned above, the conditional trust is established by Yan's message flow 300 (FIG. 3), where a challenge 302 is issued by the trustor to the trustee and a response 304 is generated by the trustee to obtain the conditional trust of the trustor. In contrast, Applicants' claim 1 is directed towards obtaining a trust-based relationship which does not require a generation of distrust signals for maintaining trust. Towards this end, a specific sequence of operations using a specific set of parameters has been recited in claim 1. Unfortunately, the Office action fails to unambiguously disclose where in the cited prior art can be found each of Applicants' claim elements (and in the order of occurrence as cited in claim 1) as is necessary for a proper rejection under 35 U.S.C. 102(e).

In this matter Applicants wish to draw attention to the Office action allegation that various elements of Applicants' claim 1 (including "*code ID*" and "*a security key included in the certificate chain*") are generally anticipated in one of the following portions of the cited prior art: *Yan paragraph [0058], lines 1-10; paragraph [0061], lines 12-16; attestation techniques utilized; paragraph [0060], lines 1-6: verify attestation message; paragraph [0060], lines 6-9; paragraph [0019], lines 10-13: modification of configuration data (attestation message information, certificate information revoked), attestation information dishonored).*

Even assuming *arguendo* that Yan anticipates (in some portion cited in the Office action) a security key of some kind, Applicants respectfully submit that the Office action still fails to unambiguously disclose where in Yan can be found Applicants' code identifier "*code ID.*" The code ID is specifically cited in claim 1 as: "*representative of the first entity...*" and the second entity is specifically cited as: "*having knowledge of each valid code ID corresponding to the first entity.*"

Applicants have provided a few examples of code ID in their original specification, for example, in paragraph [0028], which is reproduced below for easy reference:

> [0028] In one embodiment of the present invention, the code ID 16 corresponding to a particular first entity 10 is defined as a hash of the first entity 10 concatenated with the id 18 thereof. For one example, the hash may be based on any of several known SHA algorithms, including SHA-1 and SHA-256:
>
> Code ID 16 = SHA (first entity 10 | id 18)
>
> For another example, the code ID 16 may be a concatenation of two of the

aforementioned hashes, where one hash is based on SHA-1 and the other is based on SHA-256:

Code ID 16 = SHA-1 (first entity 10 1 id 18) I SHA-256 (first entity 10 1 id 18)

In light of the remarks above, Applicants respectfully submit that the current rejection of claim 1 under 35 U.S.C 102 is improper and hereby request withdrawal of the rejection followed by allowance of claim 1.

Claims 2-18

Applicants respectfully submit that claims 2-18 are allowable for several reasons and certain remarks pertaining to some of these claims have been provided below.

Additionally, Applicants respectfully submit that claims 2-12 are allowable by law arising from their dependency on allowable claim 1. *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988). Consequently, for at least this reason, Applicants respectfully request withdrawal of the rejection under 35 U.S.C. 102(e) followed by allowance of claims 2-18.

Additional remarks pertaining to some dependent claims in claims 2-18

Claim 10

The Office action rejects Applicants' claim 10 by alleging that Yan's paragraph [0062], lines 1-4 and paragraph [0064], lines 1-4 anticipate each element of the claim. Applicants respectfully traverse the rejection and submit that the cited text in Yan fails to disclose Applicants' "trust message" and further fails to disclose a shared secret incorporating a symmetric key.

Claim 11

The Office action rejects Applicants' claim 11 by alleging that Yan's paragraph [0059], lines 6-12 anticipate each element of the claim. Applicants respectfully traverse the rejection and submit that the cited text in Yan fails to disclose Applicants' "trust message" and also fails to disclose a shared secret incorporating a symmetric key. Yan further fails to disclose any of the following emphasized aspects: "*symmetric key (K) encrypted according to a public key of the first entity (PU-1)* to result in (PU-1(K)), *the second entity* obtaining (PU-1) from the *certificate chain of the* attestation message, *and wherein the first entity* obtains the symmetric key (K) *from the received* trust message *by applying* a private key (PR-1) *corresponding to (PU-1) to (PU-1(K))* to result in (K)."

Applicants respectfully request withdrawal of the rejection followed by allowance of claim 11, because the rejection fails to disclose each element of Applicants' claim 11 as is required for a proper rejection under 35 U.S.C. 102(e).

Claim 12

The Office action rejects Applicants' claim 12 by asserting that all aspects of the claim are disclosed in "*Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session key for secure communications (interaction); paragraph [0065], lines 9-15; updated attestation information (cryptographic algorithm), protocol for exchange negotiated)* (Emphasis added). Applicants respectfully traverse the rejection because Yan's "updated attestation information" (which pertains to a mistrust message generated in response to a condition change) is improperly alleged to anticipate Applicants' "*cryptographic algorithm*" of claim 12. There is no mention of a cryptographic algorithm in Yan's cited portion of text. For at least this reason, Applicants request withdrawal of the rejection followed by allowance of claim 12.

Claim 13

The Office action rejects Applicants' claim 13 by asserting that all aspects of the claim are disclosed in "*Yan paragraph [0059], lines 6-12: generate (integrity metric (code ID), attestation information).*" Applicants respectfully traverse the rejection as being improper because Yan does not anticipate that portion of claim 13 wherein the second entity constructs a trust message using the code ID of the first entity as obtained from the attestation message." For at least this reason, Applicants request withdrawal of the rejection followed by allowance of claim 13.

Claim 17

Applicants respectfully assert that the rejection is improper because it fails to accurately disclose where in Yan can be found various elements of claim 17 such as a second secret, a second trust message, and a first shared secret that is no longer valid. The sections of Yan that have been cited in the Office action fail to disclose any of these elements. Consequently, Applicants request withdrawal of the rejection followed by allowance of claim 17.

Claim 18

Claim 18 pertains to two messages - a "can-attest message" and an "attestation-wanted message." As described in Applicants' original specification (e.g. in paragraphs [0052] and [0055]), these two messages are used prior to the "attestation message."

As acknowledged in the Office action, the cited portion of Yan (paragraph [0065], lines 9-15) pertains to an "update attestation." Such a message does not anticipate either the "can-attest message" or the "attestation-wanted message" of Applicants' claim 18. Yan's update attestation, which is carried out in the form of a "mismatch message 314" is shown in Yan's Figure 3 and clearly occurs after messages 302 and 304, which represent the initial attestation between trustor and trustee (Yan paragraph [0064]), have been transacted.

Furthermore, Yan's mismatch message is initiated as well as carried out by the trustee and is not part of a two-way message transaction. Consequently, Applicants respectfully submit that the Office action improperly cites a single message ("update attestation" message) in Yan as anticipating two different messages ("can-attest message" and "attestation-wanted message") in Applicants' claim 18.

It may be further pertinent to point out that claim 18 recites: "*can-attest message stating that the first entity* can send an attestation message *but that the first entity would like to know from the second entity* whether such an attestation message is required *by such second entity and if so any requirements that such second entity has with regard to such attestation message*." Such a can-attest message is not disclosed in the cited prior art.

Applicants request withdrawal of the rejection followed by allowance of claim 18.

Independent claim 19

Applicants respectfully traverse the rejection of claim 19 under 35 U.S.C. 102(e) for several reasons. Some of the remarks (e.g. the code ID) made above with reference to the rejection of claim 1 are equally pertinent to the rejection of claim 19 though the scope of these two claims is different from one another. However, in the interests of brevity these remarks will not be repeated herein.

Applicants respectfully request withdrawal of the rejection followed by allowance of claim 19, because the rejection fails to disclose each element of Applicants' claim 19 as is required for a proper rejection under 35 U.S.C. 102(e).

Claims 20-27, 29, and 30

Applicants respectfully submit that claims 20-27, 29, and 30 are allowable for several reasons and it can be understood that some of the remarks made above with reference to dependent claims 2-18 are equally pertinent here. However, certain other remarks pertaining to some of claims 20-27, 29, and 30 have been provided below.

Nonetheless, Applicants respectfully submit that claims 20-27, 29, and 30 are also allowable by law arising from their dependency on allowable claim 19. Consequently, Applicants respectfully request withdrawal of the rejection under 35 U.S.C. 102(e) followed by allowance of claims 20-27, 29, and 30.

Claim 20

The Office action rejects Applicants' claim 20 by alleging that an "updated integrity metric" of Yan anticipates Applicants' "code ID." Applicants have provided a few examples of code ID in their original specification, for example, in paragraph [0028] reproduced below for easy reference:

> [0028] In one embodiment of the present invention, the code ID 16 corresponding to a particular first entity 10 is defined as a hash of the first entity 10 concatenated with the id 18 thereof. For one example, the hash may be based on any of several known SHA algorithms, including SHA-1 and SHA-256:
>
> Code ID 16 = SHA (first entity 10 | id 18)
>
> For another example, the code ID 16 may be a concatenation of two of the aforementioned hashes, where one hash is based on SHA-1 and the other is based on SHA-256:
>
> Code ID 16 = SHA-1 (first entity 10 1 id 18) I SHA-256 (first entity 10 1 id 18).

In light of the above, Applicants respectfully assert that the Office action allegation that an "updated integrity metric" of Yan anticipates Applicants' "code ID" is improper and hereby request withdrawal of the rejection followed by allowance of claim 20.

Claim 21

The Office action rejects Applicants' claim 21 by alleging in pertinent part that an alteration of security information in Yan causes the "code ID" to change. Allegedly, this aspect is disclosed in Yan's paragraph [0065], lines 9-15. Applicants respectfully assert that the cited portion of Yan does not disclose an alteration of security information.

Applicants respectfully request withdrawal of the rejection followed by allowance of claim 21, because the rejection fails to disclose each element of Applicants' claim 21 as is required for a proper rejection under 35 U.S.C. 102(e).

Claim 25

The Office action rejects Applicants' claim 25 by alleging in pertinent part that Yan discloses a "quoting function" that is a part of Applicants' claim 25. Allegedly, this aspect is disclosed in Yan's paragraph [0065], lines 9-15. Applicants respectfully assert that the cited portion of Yan does not disclose such a quoting function.

Applicants respectfully request withdrawal of the rejection followed by allowance of claim 25, because the rejection fails to disclose each element of Applicants' claim 25 as is required for a proper rejection under 35 U.S.C. 102(e).

Claim Rejections under 35 U.S.C. §103

I. Statement of the Rejection

Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yan in view of Qui (US PGPUB No. 20040148505).

Response to the Rejection

Claim 15

Applicants respectfully submit that claim 15 is at least allowable by law arising from dependency on allowable claim 1. *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988). Consequently, for at least this reason, Applicants respectfully request withdrawal of the rejection under 35 U.S.C. 103(a) followed by allowance of claim 15.

It may be further pertinent to point out that the cited prior art of Qui actually **teaches away** from incorporating "*an expiration time after which the shared secret and the established trust-based relationship are* no longer valid" (Applicants' claim 15). It is precisely to avoid such a condition that Qui teaches the use of "*certificates having overlapping validity*" which "*reduce/eliminate the certificate updates/downloads*..."

II. Statement of the Rejection

Claims 16, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yan in view of Grawrock (US PGPUB No. 20040117625).

Response to the Rejection

Claims 16 and 28

Applicants respectfully submit that claims 16 and 28 are at least allowable by law arising from dependency on allowable claims 1 and 19 respectively. Consequently, for at least this reason, Applicants respectfully request withdrawal of the rejection under 35 U.S.C. 103(a) followed by allowance of claims 16 and 28.

Prior Art Made of Record

The prior art made of record has been considered, but is not believed to affect the patentability of the presently pending claims.

CONCLUSION

Applicants respectfully submit that pending claims 1-30 are allowable. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned representative at (215) 568-3100.

Date: December 11, 2007

/Joseph F. Oriti/
Joseph F. Oriti
Registration No. 47,835

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439